BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC VĂN HIẾN**

-----🙞🙜🕮🙞🙜-----



**BÀI BÁO CÁO**

**NETWORKING**

**“Giám sát xây dựng và kết nối an toàn giữa các chi nhánh bằng VPN IPsec và Firewall – Ứng dụng trong hệ thống mạng doanh nghiệp”**

**TP. HỒ CHÍ MINH – 2024**

**MỤC LỤC**

[CHƯƠNG I: TỔNG QUAN VỀ MÔ HÌNH MẠNG. 3](#_Toc170905340)

[1. Giới thiệu chung 3](#_Toc170905341)

[2 Mục tiêu. 4](#_Toc170905345)

[3. Phân tích chi tiết mô hình mạng 5](#_Toc170905346)

[3.1. Kiến trúc mạng và kết nối 5](#_Toc170905347)

[3.2. Bảo mật mạng 6](#_Toc170905348)

[3.3. Quản lý và giám sát mạng 6](#_Toc170905348)

[3.4. Hiệu suất và kiểm thử 6](#_Toc170905348)

**Tổng quan về mô hình mạng kết nối các chi bằng VPn IPsec và firewall**

**1.** Giới thiệu chung

Trong thời đại công nghệ hóa, mọi lĩnh vực đều có kết nối của Internet trong công việc, chính vì vậy mà việc xây dựng hệ thống mạng LAN (mạng cục bộ) là điều thiết yếu cho các tổ chức, doanh nghiệp và cơ sơ giáo dục. Với mô hình mà chúng tôi đã xây dựng nhầm mục đích phục vụ cho các mô hình tổ chức cỡ nhỏ nhưng đầy đủ các tính năng an toàn về mạng, ứng dụng các kỹ thuật như: VLAN, định tuyến, cấp phát IP động, VPN, firewall. Và để hiểu rõ hơn về mô hình của chúng tôi với tên gọi là f , sau đây là toàn bộ những thông tin chúng tôi sẽ cung cấp cho bạn

2. Mục tiêu

Với mô hình mạng này những mục tiêu mà chúng tôi muốn hướng tới là:

- Hiệu suất cao: điều chỉnh mạng sao cho đảm bảo tốc độ truyền dữ liệu nhanh và độ trễ thấp trong mạng nội bộ.

- Bảo mật: Tăng cường bảo mật bằng cách triển khai các biện pháp bảo mật như tường lửa, VPN, và ACL để dữ liệu không bị đánh cắp và ngăn chặn truy cập trái phép.

-Khả năng mở rộng: Hệ thống mạng linh hoạt, dễ dàng kết nối cho các thiết bị mới được thêm vào mà không gặp nhiều trở ngại

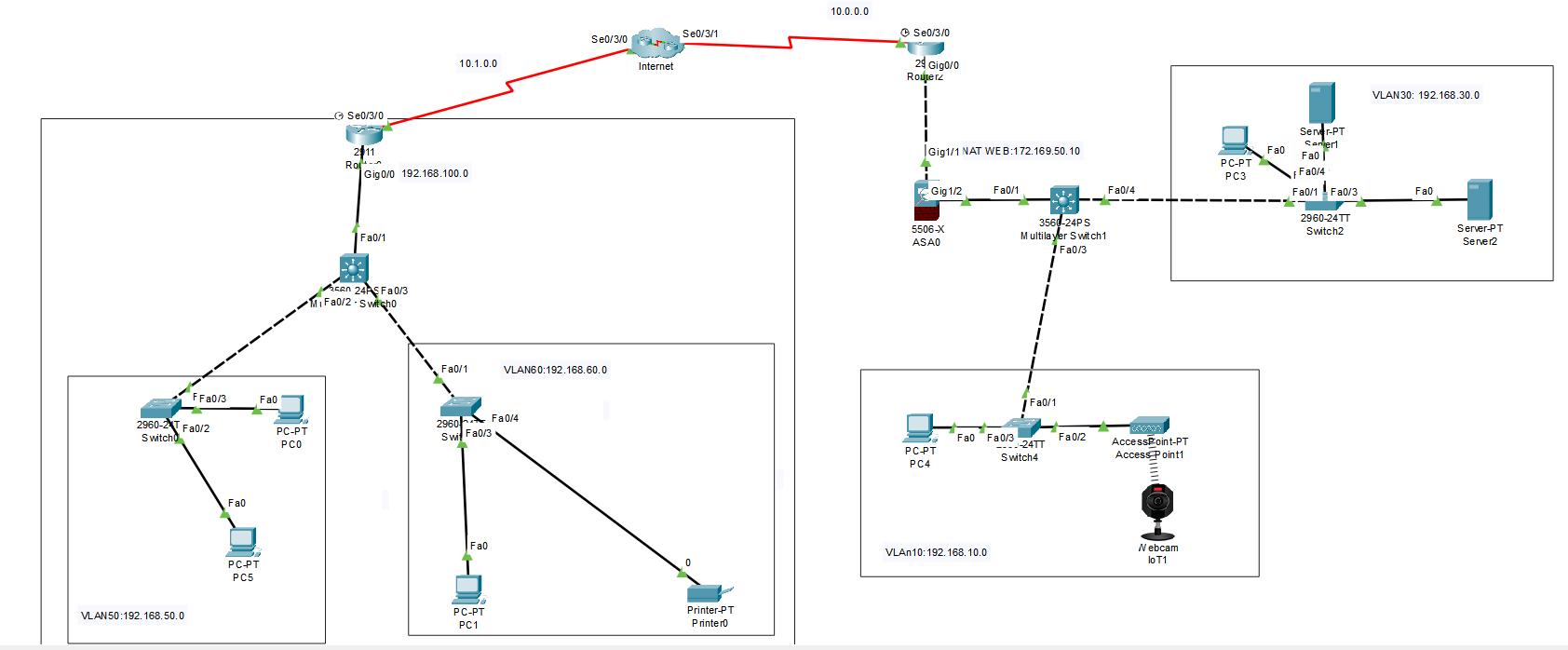
- Giám sát và quản lý: Sử dụng cấp phát IP động (DHCP) và phân vùng VLAN để đơn giản hóa quản trị mạng, tăng khả năng kiểm soát nội bộ.

- Độ an toàn: Đảm bảo hệ thống hoạt động liên tục với thời gian chết tối thiểu thông qua cấu hình dự phòng và giám sát.

3. Phân tích chi tiết mô hình mạng

Mô hình mạng được thiết kế cho một doanh nghiệp nhỏ với khoảng 20 người dùng, bao gồm các phòng ban như Kế toán, Nhân sự, và IT. Chia thành 2 khu vực là Hà Nội Và Hồ Chí Minh. Mạng được xây dựng dựa trên kiến trúc phân tầng, gồm:

* Tầng truy cập (Access Layer): Gồm các switch Cisco Catalyst 2960 hỗ trợ kết nối cho các thiết bị đầu cuối như máy tính, webcam, máy in …
* Tầng phân phối (Distribution Layer): Sử dụng switch Cisco Catalyst 3560 24-Port PoE Multilayer Switch để tổng hợp lưu lượng từ tầng truy cập và thực hiện phân vùng VLAN.
* Tầng lõi (Core Layer): Sử dụng router Cisco 2911 để xử lý định tuyến giữa các VLAN và kết nối ra Internet.
* Kết nối Internet: Một kết nối ISP được bảo vệ bởi tường lửa Cisco ASA 5516-X.



3.1. Kiến trúc mạng và kết nối

- Sử dụng VLAN để phân ra khu vực Hà Nội và Hồ Chí Minh cụ thể để dễ dàng quản lý.

- Phân vùng mạng bằng VLAN: Hệ thống mạng được chia nhỏ thành nhiều VLAN để cô lập và kiểm soát luồng dữ liệu giữa các phòng ban tại mỗi khu vực:

Hồ Chí Minh

+ VLAN10 Phòng Kế Toán

+ VLAN30 Phòng sever nội bộ

Hà Nội

+ VLAN50 Phòng Giám Đốc

+ VLAN60 Phòng Kỹ Thuật

- Việc phân chia VLAN:

+Giúp hạn chế phạm vi broadcast.

+Tách biệt dữ liệu giữa các nhóm thiết bị.

+Dễ dàng triển khai các chính sách bảo mật theo từng khu vực.

- Tại nhánh có VlAN50: sử dụng IP 192.168.50.0/24 với các thiết bị có 1 Switch và 2 PC.

- Cổng f0/1của Switch 0 L2 nhánh Hà Nội sử dụng lệnh “mode trunk” để cấu hình cổng vào chế độ trunk, cho phép truyền dữ liệu của nhiều VLAN qua một kết nối vật lý. Tại đây f0/1 kết nối đên f0/2 Switch L3.

*interface FastEthernet0/1*

*switchport mode trunk*

* Cấu hình VLAN 50 cho phòng ban Giám Đốc, cấp mạng cho các thiết bị ở khu vực.

*interface FastEthernet0/2*

*switchport access vlan 50*

*switchport mode access*

*interface FastEthernet0/3*

*switchport access vlan 50*

*switchport mode access*

- Tại nhánh có VLAN60: sử dụng IP 192.168.60.0/24 24 với các thiết bị có 1 Switch, 1 máy in và 1 PC .

- Cấu hình VLAN 60 tại Switch 1 L2, sử dụng tiếp “mode trunk” để kết nối đến Switch L3, kết nối từ f0/1 Switch 1 L2 đến f0/3 Switch L3

*interface FastEthernet0/1*

*switchport mode trunk*

* Chia VlAN60 tại Switch để cấp cho toàn phòng Kỹ Thuật

*interface FastEthernet0/3*

*switchport access vlan 60*

*switchport mode access*

*interface FastEthernet0/4*

*switchport access vlan 60*

*switchport mode access*

* Các PC và thiết bị được cấp IP động tại khu vực Hà Nội sẽ sử dụng IP động
* Để kết nối với Sever nội bộ cũng như truy cập vào Internet ta cấu hình Switch L3 tại Hà Nội

+ Bật Switch L3 để thiết bị hoạt động

*interface Vlan1*

*no ip address*

*shutdown*

+Gán địa chỉ IP các VLAN tại Switch L3 để thực hiện định tuyến giữa các VLAN , gán địa chỉ MAC. Đối với mô hình mạng này sẽ cần có sự bảo mật cũng như giám sát an ninh, kiểm soát truy cập nên sử dụng MAC tĩnh để đảm bảo độ an toàn.

*interface Vlan50*

*mac-address 000c.8585.ad01*

*ip address 192.168.50.1 255.255.255.0*

*interface Vlan60*

*mac-address 000c.8585.ad02*

*ip address 192.168.60.1 255.255.255.0*

+ Sử dụng lệnh “RIP” để trao đổi thông tin định tuyến Switch với Router 0 tại Hà Nội. Tại đây chúng tôi sử dụng “RIP version 2” vì chúng hỗ trợ:

CIDR (Classless Inter-Domain Routing) – cho phép subnet linh hoạt (VLSM).

Gửi thông tin định tuyến theo multicast 224.0.0.9 thay vì broadcast.

+ Việc sử dụng RIP version 2 sẽ giúp thiết bị tự động học đường đi đến với Router, giảm việc định tuyến thủ công.

*router rip*

*version 2*

*network 192.168.50.0*

*network 192.168.60.0*

*network 192.168.100.0*

*ip classless* // bật chế độ định tuyến không phân lớp (classless routing)

* Cấu hình DHCP:

+Khi cấu hình các địa chỉ mạng, chúng tôi sẽ giới hạn một số dãy mạng nhất định. Tại đây dãy IP từ .1 đến .10 trong dãy 192.168.50.0/24 và 192.168.60.0/24 sẽ bị loại trừ khỏi phạm vi cấp phát động của DHCP. Vì ta phải dự phòng đường mạng cho những thiết bị mới hoặc trường hợp khác.

*ip dhcp excluded-address 192.168.50.1 192.168.50.10*

*ip dhcp excluded-address 192.168.60.1 192.168.60.10*

+Cấu hình DHCP cho 2 VLAN tại Hà Nội:

*ip dhcp pool VLAN50*

*network 192.168.50.0 255.255.255.0*

*default-router 192.168.50.1*

*ip dhcp pool VLAN60*

*network 192.168.60.0 255.255.255.0*

*default-router 192.168.60.1*

* Để Switch L3 có thể thực hiện chức năng định tuyến giữa các VLAN (inter-VLAN routing), cần phải kích hoạt tính năng định tuyến IP bằng lệnh “ip routing”. Khi lệnh này được cấu hình trên Switch L3 (như thiết bị 3560-24PS trong mô hình), thiết bị sẽ có khả năng xử lý và chuyển tiếp gói tin giữa các mạng con (subnet) khác nhau, thay vì chỉ làm chức năng chuyển mạch như Switch L2

*ip routing*

* Các lệnh cấu hình VLAN10 và VLAN30 tại TP Hồ Chí Minh cũng giống như khu vực Hà Nội chỉ thay đổi dãy IP khác

+ Phòng Kế Toán với VLAN10: 192.168.10.0/24 tại Switch 2 L2

*interface FastEthernet0/1*

*switchport mode trunk*

*interface FastEthernet0/2*

*switchport access vlan 30*

*switchport mode access*

*interface FastEthernet0/3*

*switchport access vlan 30*

*switchport mode access*

+ Sever nội bộ với VLAN30:192.168.30.0/24 tại Switch 4 L2

*interface FastEthernet0/1*

*switchport mode trunk*

*interface FastEthernet0/2*

*switchport access vlan 10*

*switchport mode access*

*interface FastEthernet0/3*

*switchport access vlan 10*

*switchport mode access*

* Tại Switch L3 khu vực TP Hồ Chí Minh cũng chia rõ các dãy IP nào sẽ được cấp động và dãy IP tĩnh.

*ip dhcp excluded-address 192.168.10.1 192.168.10.10*

*ip dhcp excluded-address 192.168.20.1 192.168.20.10*

* Để các đường mạng được tối ưu hóa hơn trong mỗi VLAN, thì trong mô hình sử dụng Spanning Tree Protocol (STP):  
  spanning-tree mode pvst
* Spanning tree protocop (STP) giúp ngăn chặn việc các vòng lặp xảy ra trong hệ thống mạng LAN tại Hà Nội khi có nhiều Switch. Cũng như có cả PVST, là phiên bản mở rộng của STP, cho phép mỗi VLAN có một cây spanning riêng biệt, nhờ đó có thể cân bằng tải và tối ưu đường đi theo từng VLAN.

+Tại mỗi Switch L2 để kích hoạt mở rộng System ID trong giao thức Spanning Tree, nhằm hỗ trợ chạy Spanning Tree riêng biệt cho từng VLAN (PVST).

*spanning-tree mode pvst*

*spanning-tree extend system-id*

* Với mô hình mạng có nhiều VLAN thì việc bật PVST để

+Phân biệt từng cây spanning riêng cho mỗi VLAN.

+Hỗ trợ quá trình bầu chọn Root Bridge riêng cho từng VLAN.

+Tăng hiệu quả hoạt động của mạng và hỗ trợ cân bằng tải tốt hơn.

- Switch L3 TP Hồ Chí Minh cũng cấu hình “RIP version 2”

*router rip*

*version 2*

*network 192.168.1.0*

*network 192.168.10.0*

*network 192.168.20.0*

*network 192.168.30.0*

3.2 Bảo mật mạng

- Có sự kết hợp bảo mật từ firewall, NAT, VPN và ACL.

- Sử dụng firewall ( ASA) để kiểm soát lưu lượng mạng từ các phòng ban của các khu vực khác đi tới khu vực sever. Cấu hình ASA tại 2 điểm là g1/1 và g1/2 như sau:

*interface GigabitEthernet1/1*

*nameif outside*

*security-level 0*

*ip address 172.169.50.1 255.255.255.0*

*interface GigabitEthernet1/2*

*nameif inside*

*security-level 100*

*ip address 192.168.1.1 255.255.255.0*

* Qua cấu hình, chúng tôi cấp độ bảo mật tại TP Hồ Chí Minh là level 100 (inside) và các khu vực bên ngoài là level 0 (outside). Khi các thông tin gửi từ inside ra ngoài thì outside sẽ nhận được thông tin, nhưng quá trình ngược lại thì firewall sẽ ngăn hệ thống nhận lượng thông tin đó để bảo vệ thông và dữ liệu của inside.
* Để thông tin và dữ liệu từ khu vực Hà Nội có thể đổ về Sever nội bộ cũng như các phòng ban có kiểm soát, bảo vệ hệ thống khỏi việc bị xâm nhập trái phép. Chúng tôi đã áp dụng các chính sách kiểm soát truy cập này thông qua các danh sách điều khiển truy cập (Access Control List – ACL)

*access-list inside-out extended permit ip any any*

*access-list outside\_access\_in extended permit icmp any host 172.169.50.10*

* Như vậy thì việc trao đổi giữa các phòng ban hoạt động bình thường và không lo việc truy cập trái phép, nguy cơ tấn công từ khu vực bên ngoài.

Trong mô hình, tại dòng lênh “ access-list outside\_access\_in extended permit icmp any host 172.169.50.10” cho phép người dùng bên ngoài có thể truy cập vào Web Server nội bộ một cách an toàn và kiểm soát, hệ thống sử dụng kỹ thuật NAT tĩnh trên thiết bị tường lửa ASA. Cấu hình được thực hiện như sau:

*object network WEB*

*host 192.168.30.20*

*nat (inside,outside) static 172.169.50.10*

* Lệnh trên ánh xạ địa chỉ IP nội bộ 192.168.30.20 (Web Server) với địa chỉ công khai 172.169.50.10. Khi người dùng từ Internet truy cập IP công khai này, ASA sẽ tự động chuyển tiếp lưu lượng đến Web Server trong VLAN30. Việc này cho phép công bố dịch vụ ra bên ngoài một cách an toàn và kiểm soát, đặc biệt khi kết hợp với ACL để lọc truy cập.
* Việc sử dụng NAT tĩnh giúp công bố dịch vụ nội bộ ra ngoài Internet mà không cần đặt trực tiếp server ra vùng DMZ, đồng thời vẫn đảm bảo an toàn thông qua kiểm soát truy cập bằng ACL. Đây là phương pháp phổ biến và hiệu quả để chia sẻ tài nguyên nội bộ như Web Server, FTP, hoặc dịch vụ API cho bên ngoài một cách bảo mật và rõ ràng.
* Sử dụng “Router RIP” để định tuyến

*router rip*

*version 2*

*network 172.169.0.0*

*network 192.168.1.0*

* Tại 2 router kết nối của 2 khu vực đến Internet, cấu hình chính sách VPN IPsec Site-to-Site:

*crypto isakmp policy 10*

*encr aes*

*authentication pre-share*

*group 2*

* Cấu hình ISAKMP Policy (Phase 1) dùng để thiết lập thông số thương lượng ban đầu giữa hai thiết bị VPN.

+ crypto isakmp policy 10: Tạo policy số 10 để xác định thứ tự ưu tiên khi so sánh với các peer.

+encr aes: Sử dụng thuật toán mã hóa AES

+authentication pre-share: Xác thực bằng khóa chia sẻ trước (pre-shared key), tức là cả hai bên phải cấu hình cùng một mật khẩu.

+group 2: Sử dụng nhóm Diffie-Hellman Group 2 để trao đổi khóa (mức bảo mật trung bình, 1024-bit).

*crypto isakmp key vpn123 address 10.1.0.2*

* Khóa bị mật là vpn123 và chúng sẽ được xác thực tại địa chỉ 10.1.0.2, tức là địa chỉ cổng WAN của đối tác.
* Giúp hai router tin tưởng nhau trước khi tạo kênh mã hóa IPsec. Nếu pre-shared key không khớp, VPN sẽ không được thiết lập.
* Để bảo vệ dữ liệu truyền qua Internet giữa hai chi nhánh, mô hình đã triển khai giải pháp VPN IPsec Site-to-Site. Phía router trung tâm được cấu hình sử dụng giao thức ISAKMP (Phase 1) và IPsec (Phase 2) để mã hóa kết nối. Cụ thể:

crypto ipsec transform-set TS esp-aes esp-sha-hmac

* Dòng lệnh này tạo một transform-set tên TS, sử dụng thuật toán AES để mã hóa dữ liệu và SHA để kiểm tra tính toàn vẹn gói tin. Đây là phần cấu hình cho Phase 2 của IPsec, nơi dữ liệu thực được mã hóa khi truyền đi.

*crypto map VPN-MAP 10 ipsec-isakmp*

*set peer 10.1.0.2*

*set transform-set TS*

*match address 110*

* Khối lệnh này định nghĩa một crypto map tên VPN-MAP, thiết lập địa chỉ peer là 10.1.0.2 – IP router bên chi nhánh. Dữ liệu được mã hóa sẽ tuân theo transform-set TS, và chỉ áp dụng cho các gói tin khớp với Access Control List (ACL) số 110. ACL này thường xác định lưu lượng giữa hai mạng nội bộ, ví dụ từ 192.168.50.0/24 đến 192.168.60.0/24.
* Mỗi dòng xác định một cặp mạng nguồn → đích được cho phép truyền qua VPN tunnel.

*access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255*

*access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255*

*access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255*

*access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.100.0 0.0.0.255*

*access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255*

*access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255*

*access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.100.0 0.0.0.255*

*access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255*

*access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255*

* Xác định rõ phạm vi dữ liệu sẽ đi qua VPN IPsec, giúp giảm thiểu việc mã hóa không cần thiết.
* Tăng tính bảo mật bằng cách chỉ cho phép các VLAN nội bộ liên lạc với nhau qua kết nối bảo mật.
* Hạn chế truy cập không mong muốn hoặc sai mục đích đến các vùng mạng nội bộ khác.

3.3 Quản lý và giám sát mạng

- Ở tầng phân phối có các Switch layer 3 quản lý các VLAN, việc chia các thiết bị theo từng VLAN nhầm tăng việc bố trí đồng đều trong việc giám sát cũng như cân bằng các thiết bị

- Thiết bị cố định (PC, Server, Printer): Đặt IP tĩnh trong cấu hình thiết bị.

* Thiết bị di động (IoT, wireless): Có thể cấp phát IP qua DHCP (trên router hoặc ASA).
* Cổng liên kết (switch, router, ASA): Gán IP tĩnh trong các dải quản lý.
* Tại các phòng ban đều có kết nối về các Router định tuyến cho phép truy cập được vào Internet qua sự kiểm soát của firewall.
* Sử dụng bảng theo dõi IP (IP Plan) trên file Excel hoặc phần mềm quản lý như:

+ phpIPAM

+SolarWinds IP Address Manager

3.4 Hiệu suất và kiểm thử

- Phương pháp kiểm tra kết nối, độ trễ, và bảo mật.

- Kết quả đánh giá hiệu suất mạng.

- Triển khai và cấu hình thiết bị

- Cấu hình chi tiết của switch, router, và firewall.

- Quy trình triển khai phần cứng và phần mềm.

**Kết luận**

**Điểm mạnh:** Bố cục này nhấn mạnh các chức năng cốt lõi của mạng, giúp người đọc dễ dàng tập trung vào các khía cạnh như bảo mật hoặc quản lý. Nó phù hợp khi trình bày cho các nhà quản lý kỹ thuật hoặc đội ngũ IT.

Báo cáo đã trình bày quá trình thiết kế và triển khai một mạng doanh nghiệp nhỏ, tích hợp các công nghệ LAN, định tuyến, DHCP, VPN IPsec, tường lửa, và ACL. Mạng đáp ứng các mục tiêu về hiệu suất, bảo mật, và khả năng mở rộng. Các bài học kinh nghiệm bao gồm tầm quan trọng của phân vùng VLAN để quản lý lưu lượng và cần thiết phải kiểm tra bảo mật định kỳ. Trong tương lai, mạng có thể được nâng cấp với các tính năng như QoS để ưu tiên lưu lượng và giám sát mạng thời gian thực.